

ASSOCIATIVE AND JORDAN ALGEBRAS GENERATED BY TWO IDEMPOTENTS

LOUIS ROWEN¹ YOAV SEGEV

ABSTRACT. The purpose of this note is to obtain precise information about associative or Jordan algebras generated by two idempotents.

1. INTRODUCTION

This paper is motivated by recent work on commutative nonassociative algebras generated by idempotents. Such algebras are for example the Griess algebras associated with vertex operator algebras, and Majorana algebras [I, Ma, Mi, Sa]. Also Jordan algebras generated by idempotents as well as Axial algebras ([HRS1, HRS2, HSS]) are such, see also [DeMR].

In these algebras the adjoint operator associated to the generating idempotents (i.e., multiplication by the idempotent) is semi-simple and has few eigenvalues. Further, certain fusion rules (i.e., multiplication rules), between the eigenspaces are assumed (similar to the Peirce decomposition multiplication rules in Jordan algebras, see e.g., [ZSSS, Theorem 4, p. 334]). One can then associate an involutive automorphism of the algebra to each of these idempotents, and the group generated by these involutions are sometimes of great interest (e.g., the Monster group).

In general, it is not unintuitive to think about idempotents in these algebras in a similar way one thinks of involutions in a group. In all these algebras it is important to know the subalgebras generated by two idempotents. Some papers dealt with this question in the associative case (e.g. [B, L, V]), and some in the Jordan algebra case (e.g. [HRS2, Sa]).

Throughout \mathbb{F} is a unital commutative ring. Let A be a (linear) algebra over \mathbb{F} with multiplication denoted by $u \circ v$, $u, v \in A$, so if A is a ring we take $\mathbb{F} = \mathbb{Z}$, the integers. We let $A^{(1)}$ be the algebra A if A is unital (i.e. A has an identity element), and $A^{(1)} = \mathbb{F} \oplus A$ with multiplication defined by

$$(\alpha, x)(\beta, y) = (\alpha\beta, \alpha y + \beta x + x \circ y),$$

if A does not have an identity element. In the latter case $A^{(1)}$ has the identity element $\mathbb{1} = (1, 0)$. We identify A with the subset $\{(0, x) \mid x \in A\}$

Date: September 19, 2016.

2000 Mathematics Subject Classification. Primary: 16S15, 17C27.

Key words and phrases. idempotents, associative algebra, Jordan algebra.

¹Partially supported by the Israel Science Foundation grant no. 1623/16.

of $A^{(1)}$. Thus $\mathbb{1}$ denotes the identity element of $A^{(1)}$ (also in the case where A is unital).

For an element $x \in A$ we let $x^0 = \mathbb{1} \in A^{(1)}$. The cases that will interest us in this note are the case where A is associative, and the case where $A = J$ is a Jordan algebra, and \mathbb{F} is a field of characteristic not 2. In both cases, A is *power associative*, and we let, as usual, $\mathbb{F}[x] \subseteq A^{(1)}$ be the subalgebra of $A^{(1)}$ generated by x over \mathbb{F} , i.e., the set of polynomials in x with coefficients in \mathbb{F} .

Some parts of our first theorem are mostly known in principle:

Theorem 1.1. *Let A be an associative algebra (not necessarily with $\mathbb{1}$) over a unital commutative ring \mathbb{F} , generated by two distinct idempotents a and b . Denote multiplication in A by **juxtaposition**: xy . Then*

- (1) ([B, §12.2], [L, Lemma 3]) $\sigma := (a - b)^2$ is in the center of A .
- (2) A is spanned by σ, a, b and ab as a module over $\mathbb{F}[\sigma]$. In particular A satisfies a multilinear polynomial identity.
- (3) If $\sigma = \mathbb{1}$, then $aba = bab = 0$. Hence either $ab = ba = 0$ and $A = \mathbb{F}a \oplus \mathbb{F}b$, or one of $\mathbb{F}(ab)$ or $\mathbb{F}(ba)$ is a nontrivial square-zero ideal of A .
- (4) If $\sigma = 0$, then one of $\mathbb{F}(a(b - \mathbb{1})) + \mathbb{F}(b(a - \mathbb{1}))$ or $\mathbb{F}(a - b)$ is a nontrivial square-zero ideal of A .
- (5) In both cases (3) and (4), A has a nilpotent ideal I such that A/I is commutative. In case (3) we can take $I^2 = 0$, and in case (4) we can take $I^3 = 0$.
- (6) If $\sigma - \sigma^2$ is invertible in A (so that $\mathbb{1} \in A$), then $A \cong M_2(\mathbb{F}[\sigma])$. In particular, if $\mathbb{F}[\sigma]$ is a field (so that $\mathbb{F}\mathbb{1}$ is a field and σ is algebraic over $\mathbb{F}\mathbb{1}$), with $\sigma \neq 0, \mathbb{1}$, then $A \cong M_2(\mathbb{F}[\sigma])$.
- (7) (Compare with [L, Theorem 4].) If A is simple, then $\mathbb{1} \in A$ and $\mathbb{F}[\sigma]$ is a field (so $\mathbb{F}\mathbb{1}$ is a field and σ is algebraic over $\mathbb{F}\mathbb{1}$). Further, either $A = \mathbb{F}\mathbb{1}$ is a field (and $\{a, b\} = \{0, \mathbb{1}\}$) or $A \cong M_2(\mathbb{F}[\sigma])$.
- (8) Let $J = \mathbb{F}[\sigma]\sigma + \mathbb{F}[\sigma]a + \mathbb{F}[\sigma]b$. Then there is an involution $*$ on A defined by:

$$(\alpha_\sigma\sigma + \alpha_a a + \alpha_b b + \alpha_{ab}(ab))^* = \alpha_\sigma\sigma + \alpha_a a + \alpha_b b + \alpha_{ab}(ba)$$

if and only if

$$(i) \quad \alpha(ab) \in J, \text{ for some } \alpha \in \mathbb{F}[\sigma] \implies \alpha(ba - ab) = 0.$$

In particular, if A is simple and not commutative, then $*$ is an involution on A .

(See also Theorem 3.5 for additional significant information.)

For the notion of the *center* of a Jordan algebra, see Definition 2.1(5) below.

Theorem 1.2. *Let J be a Jordan algebra over a field \mathbb{F} of characteristic not 2 generated by two distinct idempotents a and b . Denote the multiplication in J by **dot**: $x \cdot y$. Then*

- (1) $\sigma := (a - b)^2$ is in the center of J ;

- (2) J is spanned by a, b , and σ as a module over $\mathbb{F}[\sigma]$;
- (3) if the Jordan algebra J is simple, then either $J = \mathbb{F}$ or $J \cong \mathcal{H}(A, *)$ the set of symmetric elements $x^* = x$, where A is a **simple** algebra as in Theorem 1.1(7), and $*$ is as in Theorem 1.1(8). (Of course $\mathcal{H}(A, *)$ is a subalgebra of A^+).

2. PROOFS OF THEOREM 1.1 AND THEOREM 1.2

Before we prove Theorems 1.1 and 1.2 we need a few definitions, the statement of the Shirshov-Cohn Theorem, and a few lemmas.

- Definitions 2.1.**
- (1) A (linear) algebra is just an algebra over a commutative unital ring \mathbb{F} in the usual sense (but not necessarily associative).
 - (2) For an algebra (A, \circ) , the *commutator* is $[x, y] := x \circ y - y \circ x$ and the *associator* is $[x, y, z] := (x \circ y) \circ z - x \circ (y \circ z)$.
 - (3) The *nucleus* of an algebra is the part that associates with everything, consisting of the elements associating in all possible ways with all other elements:

$$\mathcal{Nuc}(A) := \{x \in A \mid [x, A, A] = [A, x, A] = [A, A, x] = 0\}.$$

- (4) The *center* of any algebra is the part of the algebra which both commutes and associates with everything, i.e., those nuclear elements commuting with all other elements:

$$\text{Cent}(A) := \{c \in \mathcal{Nuc}(A) \mid [c, A] = 0\}.$$

- (5) Recall that for an associative algebra A , the Jordan algebra A^+ is defined by $x \cdot y = \frac{1}{2}(xy + yx)$. Any subalgebra of a Jordan algebra of type A^+ is called *special*.

Theorem 2.2 (Shirshov-Cohn Theorem, Theorem 10, p. 48 in [J]). *Any Jordan algebra over a field \mathbb{F} of characteristic not 2 (with $\mathbb{1}$) generated by two elements (and $\mathbb{1}$) is special.*

Notation 2.3. From now on we fix two *distinct* idempotents a, b in the algebra A over a unital commutative ring \mathbb{F} (A will be either associative, or $A = J$ a Jordan algebra, and then \mathbb{F} is a field of characteristic not 2). We assume that A is generated by a and b as an algebra over \mathbb{F} (but we do not assume that A is unital). Let

$$\sigma := (a - b)^2 = a + b - (ab + ba).$$

We need a few computations.

Lemma 2.4. *Assume that A is associative (so multiplication in A is denoted: xy).*

- (1) $\sigma a = a - aba = a\sigma$.
- (2) $\sigma b = b - bab = b\sigma$.

- (3) $aba = (\mathbb{1} - \sigma)a$ and $bab = (\mathbb{1} - \sigma)b$.
- (4) $(\mathbb{1} - a)(\mathbb{1} - b)(\mathbb{1} - a) = (\mathbb{1} - \sigma)(\mathbb{1} - a)$ and $(\mathbb{1} - b)(\mathbb{1} - a)(\mathbb{1} - b) = (\mathbb{1} - \sigma)(\mathbb{1} - b)$.

Proof. We have $\sigma a = (a + b - ab - ba)a = a + ba - aba - ba = a - aba$. Also $a\sigma = a(a + b - ab - ba) = a + ab - ab - aba = a - aba$. Hence (1) holds. Part (2) holds by symmetry. Part (3) follows from (1) and (2). For part (4) notice that $x := \mathbb{1} - a$ and $y := \mathbb{1} - b$ are idempotents in $A^{(1)}$ and $(x - y)^2 = \sigma$. Hence, as in (3), we get (4). \square

Lemma 2.5. *Assume that A is associative and commutative. Then*

- (1) $\sigma(a - b) = a - b$, in particular $\sigma^2 = \sigma$;
- (2) $\sigma ab = 0$;
- (3) $A = \mathbb{F}\sigma a \oplus \mathbb{F}\sigma b \oplus \mathbb{F}ab$.

Proof. We use Lemma 2.4. We have $ab = aba = a - \sigma a$. Similarly $ba = b - \sigma b$. Hence $a - \sigma a = b - \sigma b$, so $a - b = \sigma(a - b)$, and the first part of (1) holds. Multiplying by $a - b$ we get (1). Also $ab = (ab)b = ab - \sigma ab$, so $\sigma ab = 0$, and (2) holds.

Let W be the \mathbb{F} -linear combination of $\sigma a, \sigma b$ and ab . Then $a = ab + \sigma a \in W$ and similarly $b \in W$. Clearly, by (2), W is closed under multiplication, so $W = A$. Suppose $\alpha(\sigma a) + \beta(\sigma b) + \gamma(ab) = 0$, with $\alpha, \beta, \gamma \in \mathbb{F}$. Multiplying by σa and using (1) and (2) we get that $\alpha(\sigma a) = 0$. Similarly $\beta(\sigma b) = 0$, and then $\gamma(ab) = 0$. Also, by (2), the sum is a direct sum of ideals, so (3) holds. \square

In the next lemma, by a simple ring R we mean a ring (not necessarily unital) such that $R^2 \neq 0$ and the only proper ideal of R is $\{0\}$. This lemma is well known. We include a proof for the convenience of the reader.

Lemma 2.6. *Let R be a simple ring that satisfies a polynomial identity. Then $R \cong M_n(D)$, for some division ring D . In particular R is unital.*

Proof. We show that R is contained as an ideal in a unital primitive ring S that satisfies a (multilinear) polynomial identity. By Kaplansky's Theorem [R, Theorem 23.31], S is a simple ring which is finite dimensional over its center (which is a field). Since S is simple and since R is an ideal of S we have $R = S$. By Wedderburn's Theorem $R \cong M_n(D)$ as asserted.

If R is unital, take $S = R$ (a simple unital ring is primitive). So suppose R is not unital. Now R is an algebra over the integers and we let $R^{(1)}$ be the ring defined above (adjoining an identity $\mathbb{1}$ to R). We identify R with the ideal $\{(0, r) \mid r \in R\}$. Consider the Jacobson Radical $J(R^{(1)})$. Since R is an ideal of $R^{(1)}$ we have $J(R) = J(R^{(1)}) \cap R$ ([Her, Theorem 1.2.5]). Hence if $J(R^{(1)}) \supseteq R$, then $J(R) = R$ (i.e. R is a radical ring). However, by [Ja, Theorem 4.2], since R satisfies a polynomial identity, $J(R) \neq R$. Since R is simple, we see that $R \cap J(R^{(1)}) = \{0\}$.

Let $S := R^{(1)}/J(R^{(1)})$. Then R embeds in S and we consider R as a subring of S . Since $J(S) = \{0\}$, and since $J(S)$ is the intersection of all

primitive ideals of S , there exists a primitive ideal P of S that does not contain R , and hence intersects R in $\{0\}$. Replacing S by S/P we may assume that S is primitive. Now since R satisfies a polynomial identity, it satisfies a multilinear polynomial identity ([Her, Lemma 6.2.4]). Since S is a central extension of R , [R, Proposition 23.8(i)] shows that S satisfies a multilinear polynomial identity, so we are done. \square

Proof of Theorem 1.1. (1): This follows from Lemma 2.4(1&2).

(2): Let

$$V = \mathbb{F}[\sigma]\sigma + \mathbb{F}[\sigma]a + \mathbb{F}[\sigma]b + \mathbb{F}[\sigma]ab,$$

the set of $\mathbb{F}[\sigma]$ linear combinations of σ, a, b and ab . We show that V is a subalgebra of A . Since it contains a and b , this will show that $A = V$.

Since $\sigma \in \text{Cent}(A)$ to show that V is a subalgebra of A it suffices to show that $ba, aba, bab \in V$, but this follows from Lemma 2.4, and from the fact that $ba = -\sigma + a + b - ab$. The last part of (2) follows from [R, Proposition 23.11].

(3): Suppose $\sigma = 1$. By Lemma 2.4(3), $aba = bab = 0$. If $ab = ba = 0$ then it is easy to check that $A = \mathbb{F}a \oplus \mathbb{F}b$. Suppose $ab \neq 0$. Then $(ab)^2 = 0$ and we see that $\mathbb{F}(ab)$ is closed under multiplication by a and b from both sides, so (3) holds.

(4): Suppose $\sigma = 0$. Then, by Lemma 2.4(3), $aba = a$ and $bab = b$. Let $x := a(1 - b), y := b(1 - a)$ and $I := \mathbb{F}x + \mathbb{F}y$. If $x = y = 0$, then since $a - b \neq 0$, we see that $\mathbb{F}(a - b)$ is a nontrivial square-zero ideal. Assume $x \neq 0$. Then $bx = ba(1 - b) = ba - b = -y$, $xb = 0, ax = x$ and $xa = 0$. Similarly $ay, ya, by, yb \in I$. Also $x^2 = y^2 = xy = yx = 0$. Hence $I^2 = \{0\}$ and (4) holds.

(5): In (3) we take $I = \mathbb{F}ab + \mathbb{F}ba$. In (4) if $x = y = 0$ we take $I = \mathbb{F}(a - b)$, since then the images of a and b are equal. So suppose $x \neq 0$. Let $z = ab - ba$ and take $I = \mathbb{F}(x + y) + \mathbb{F}z$. Note that ab and ba are idempotents and since $vvv = v$, for $\{v, w\} = \{a, b\}$, we see that $z^2 = ab - a + ba - b = -x - y$. It is easy to check that $zx = x + y, xz = 0, zy = -x - y$ and $yz = 0$. Hence $I^2 = \mathbb{F}(x + y)$. Now, by the above, and by the proof of (4), $I(x + y) = (x + y)I = \{0\}$. Hence $I^3 = \{0\}$, and A/I is abelian.

(6): Set $e_{1,1} = a, e_{1,2} = ab(1 - a), e_{2,1} = (\sigma(1 - \sigma))^{-1}(1 - a)ba$ and $e_{2,2} = 1 - a$. Then

$$e_{1,1}e_{i,j} = \delta_{1,i}e_{1,j} \quad \text{and} \quad e_{2,2}e_{i,j} = \delta_{2,i}e_{2,j}.$$

Also,

$$e_{1,2}e_{1,1} = 0 = e_{1,2}e_{1,2} \quad \text{and} \quad e_{2,1}e_{2,2} = 0 = e_{2,1}e_{2,1}.$$

Next, using Lemma 2.4(1&3),

$$\begin{aligned} \sigma(1 - \sigma)e_{1,2}e_{2,1} &= ab(1 - a)ba = aba - ababa \\ &= aba - ab(a - \sigma a) = \sigma aba = \sigma(1 - \sigma)a, \end{aligned}$$

Since $\sigma(1 - \sigma)$ is invertible in A we get $e_{1,2}e_{2,1} = a = e_{1,1}$.

Similarly, using Lemma 2.4(3&4),

$$\begin{aligned}\sigma(1 - \sigma)e_{2,1}e_{1,2} &= (1 - a)bab(1 - a) = (1 - a)(b - \sigma b)(1 - a) \\ &= (1 - \sigma)(1 - a)(1 - b)(1 - a) = \sigma(1 - \sigma)(1 - a),\end{aligned}$$

Since $\sigma(1 - \sigma)$ is invertible in A we get $e_{2,1}e_{1,2} = e_{2,2}$. Thus the $e_{i,j}$ are 2×2 matrix units generating A over $\mathbb{F}[\sigma]$ (see Definition 13.3 in [R]). By [R, Proposition 13.9], $A \cong M_2(R)$, where $R = aAa$. Since $aba = (1 - \sigma)a$ (Lemma 2.4(3)), and by part (2), $R = \mathbb{F}[\sigma]a$. Note now that $\mathbb{F}[\sigma]a \cong \mathbb{F}[\sigma]$, because if $\alpha a = 0$, for some $\alpha \in \mathbb{F}[\sigma]$, then $e_{2,1}\alpha ae_{1,2} = \alpha e_{2,2} = \alpha(1 - a) = 0$, and then $\alpha = 0$. Hence the map $\alpha \mapsto \alpha a$ is an isomorphism $\mathbb{F}[\sigma] \rightarrow R$ and (6) holds.

(7): Suppose next that A is simple. We may assume without loss that $a \neq 0$. If A is commutative, then $A = Aa$, and $a = 1$ is the identity of A . Thus A is a field so $b = 0$ and it follows that $A = \mathbb{F}1$.

Suppose that A is not commutative. If A is a division ring, then $\{a, b\} = \{1, 0\}$ and $A = \mathbb{F}1$ is commutative, a contradiction.

By (2), A satisfies a multilinear polynomial identity. By Lemma 2.6, $1 \in A$, and $A \cong M_n(D)$ for some division ring D . Let $\mathbb{K} := \text{Cent}(A)$. Then \mathbb{K} is a field, and by (2) the dimension of A over \mathbb{K} is at most 4. Since this dimension is a square which is not 1, it is 4.

Hence $\{\sigma, a, b, ab\}$ are linearly independent over \mathbb{K} . It follows that $\{\sigma, a, b, ab\}$ are linearly independent over $\mathbb{F}[\sigma] \subseteq \mathbb{K}$. Now if σ is transcendental over \mathbb{F} , then $\mathbb{F}[\sigma]$ has a proper non-trivial ideal I . And then $I\sigma + Ia + Ib + I(ab)$ would be a proper nontrivial ideal of A , a contradiction. Hence $\mathbb{F}[\sigma]$ is a field. Since A is simple and contains idempotents, $\sigma \notin \{0, 1\}$, by (3) and (4). Hence $\sigma - \sigma^2$ is invertible in A , so $A \cong M_2(\mathbb{F}[\sigma])$ by (6).

(8): Suppose that $*$ is an involution on A . Assume that $\alpha_\sigma\sigma + \alpha_a a + \alpha_b b + \alpha_{ab}(ab) = 0$. Then also $\alpha_\sigma\sigma + \alpha_a a + \alpha_b b + \alpha_{ab}(ba) = 0$. Subtracting we get $\alpha_{ab}(ba - ab) = 0$. Thus condition (i) of (8) holds.

Suppose condition (i) of (8) holds, and assume that

$$\alpha_\sigma\sigma + \alpha_a a + \alpha_b b + \alpha_{ab}(ab) = 0.$$

Then

$$\begin{aligned}\alpha_\sigma\sigma + \alpha_a a + \alpha_b b + \alpha_{ab}(ba) &= \\ \alpha_\sigma\sigma + \alpha_a a + \alpha_b b + \alpha_{ab}(ab) + \alpha_{ab}(ba - ab) &= \alpha_{ab}(ba - ab).\end{aligned}$$

By condition (i), $\alpha_{ab}(ba - ab) = 0$, so $\alpha_\sigma\sigma + \alpha_a a + \alpha_b b + \alpha_{ab}(ba) = 0$. This shows that $*$ is well defined, and it is easy to check that it is an involution on A .

For the last part of (8), see Remark 2.7(3) below and note that $\mathbb{F}[\sigma]$ is a field, and A is 4-dimensional over $\mathbb{F}[\sigma]$. \square

Remarks 2.7. (1) By [L, Theorem 4], the converse of Theorem 1.1(3) also holds, namely if $A = M_2(\mathbb{K})$ where \mathbb{K} is a finite simple field

extension of \mathbb{F} , then A is generated over \mathbb{F} by two idempotents, except in the case where $\mathbb{K} = \mathbb{F}_2$, the field of two elements.

- (2) Suppose that $ab = 0$. Then, by Lemma 2.4(1&2), $\sigma = 1$, and then $ba = -1 + a + b$. Note that $1(ba - ab) = ba$, is not necessarily 0, so it may happen that $*$ of Theorem 1.1(8) is not an involution on A .
- (3) Of course if $\{\sigma, a, b, ab\}$ are independent over $\mathbb{F}[\sigma]$ then $*$ of Theorem 1.1(8) is an involution on A .

Proof of Theorem 1.2. By the Shirshov-Cohn theorem, J is a special algebra contained in A^+ , where A is an associative algebra generated over \mathbb{F} by the idempotents a and b .

(1): This follows immediately from Theorem 1.1(1).

(2): By (1), and since $a \cdot b = -\frac{1}{2}(\sigma + a + b)$, it follows that the set of $\mathbb{F}[\sigma]$ -linear combinations of σ, a, b is closed in J under multiplication, and hence it is equal to J .

(3): Assume that J is simple. If A is commutative, then $J = A$ is a field, so $J = \mathbb{F}$. So assume that A is not commutative. Let I be a maximal ideal of A not containing J . Since J is simple, $J \cap I = \{0\}$. Hence we may replace A with the simple associative algebra A/I . Hence we may assume that A is simple. By Theorem 1.1(8), $*$ is an involution on A , and one easily checks that $J = \mathcal{H}(A, *)$. \square

3. SOME ADDITIONAL RESULTS FOR THE CASE WHERE \mathbb{F} IS A FIELD AND A IS ASSOCIATIVE

In this section we continue with Notation 2.3. We further assume that A is associative and that \mathbb{F} is a field.

Proposition 3.1. *Exactly one of the following holds:*

- (a) A is finite dimensional over \mathbb{F} , and σ is algebraic over \mathbb{F} (i.e. it satisfies a polynomial in $\mathbb{F}[\lambda]$), or
- (t) A is infinite dimensional over \mathbb{F} and σ is transcendental over \mathbb{F} . In this case A is isomorphic to the semigroup algebra of the free product $\langle a \rangle * \langle b \rangle$ of the one-element semigroups $\langle a \rangle, \langle b \rangle$.

Proof. If A is finite dimensional over \mathbb{F} , then (a) holds, while if A is infinite dimensional over \mathbb{F} then, by [L, Proposition 2], A is as in (t).

Suppose A is as in (t). Then a direct and easy computation, based on the leading term starting with ab (or ba), shows that $\sigma = a + b - ab - ba$ cannot satisfy a polynomial over \mathbb{F} . \square

Lemma 3.2. *Let $g_1, g_2 \in \mathbb{F}[\lambda]$ be relatively prime polynomials such that $g_1[\sigma]g_2[\sigma] = 0$. Then $A \cong A/Ag_1[\sigma] \times A/Ag_2[\sigma]$.*

Proof. This follows from the Chinese Remainder Theorem, whose argument we review since we need it for algebras without $\mathbb{1}$. First note that $Ag_i[\sigma]$ is an ideal of A since $g_i[\sigma]$ is central in $A^{(1)}$.

Now if $r \in Ag_1[\sigma] \cap Ag_2[\sigma]$ then $rg_2[\sigma] = rg_1[\sigma] = 0$, so writing

$$a_1[\lambda]g_1[\lambda] + a_2[\lambda]g_2[\lambda] = 1,$$

for $a_1, a_2 \in \mathbb{F}[\lambda]$, we see that $r = ra_1[\sigma]g_1[\sigma] + ra_2[\sigma]g_2[\sigma] = 0$, implying $A \hookrightarrow A/Ag_1[\sigma] \times A/Ag_2[\sigma]$. On the other hand, for any $r_1 + Ag_1[\sigma] \in A/Ag_1[\sigma]$ and $r_2 + Ag_2[\sigma] \in A/Ag_2[\sigma]$ we take

$$r = r_1a_2[\sigma]g_2[\sigma] + r_2a_1[\sigma]g_1[\sigma],$$

and note that

$$r + Ag_1[\sigma] = r_1a_2[\sigma]g_2[\sigma] + Ag_1[\sigma] = r_1(1 - a_1[\sigma]g_1[\sigma]) + Ag_1[\sigma] = r_1 + Ag_1[\sigma]$$

and likewise $r + Ag_2[\sigma] = r_2 + Ag_2[\sigma]$. \square

Proposition 3.3. *Let $g[\lambda] \in \mathbb{F}[\lambda]$ be irreducible, let $k \geq 1$ and let $h[\lambda] = g[\lambda]^k$. Suppose that $Ah[\sigma] \neq A$, and let $\bar{A} = A/Ah[\sigma]$. Let $\bar{\sigma}$ be the image of σ in $A/Ah[\sigma]$. Then*

- (1) *If $g[\lambda] = \lambda$, then $\bar{\sigma}$ is nilpotent in \bar{A} , and there exists a nilpotent ideal \bar{J} in \bar{A} such that \bar{A}/\bar{J} is abelian.*
- (2) *If $g[\lambda] \neq \lambda$, then \bar{A} is unital, furthermore $\bar{\sigma}$ is invertible in \bar{A} . Denote by \bar{e} the identity element of \bar{A} . Then $h[\bar{\sigma}] = \bar{0}$ (where we substitute 1 by \bar{e} in $h[\bar{\sigma}]$).*
- (3) *If $g[\lambda] = \lambda - 1$, then $\bar{\sigma} - \bar{e}$ is nilpotent in \bar{A} and there exists a nilpotent ideal \bar{J} in \bar{A} such that \bar{A}/\bar{J} is abelian.*
- (4) *If $g[\lambda]$ is relatively prime to $\lambda(\lambda - 1)$, then, by (2), \bar{A} is unital, and $\bar{A} \cong M_2(\mathbb{F}[\bar{\sigma}])$.*

Proof. (1): Suppose that $g[\lambda] = \lambda$. Then $Ah[\sigma] = A\sigma^k$, so the ideal $\bar{I} := A^{(1)}\sigma/A\sigma^k$ is a nilpotent ideal in \bar{A} . Indeed

$$\left(A^{(1)}\sigma\right)^{k+1} = \left(A^{(1)}\sigma\right)A^{(1)}\sigma^k \subseteq AA^{(1)}\sigma^k = A\sigma^k.$$

Also in the algebra $\bar{A}/\bar{I} \cong A/A^{(1)}\sigma$ the image of σ is 0. Hence by Theorem 1.1(5), the algebra \bar{A}/\bar{I} has a nilpotent ideal over which it is commutative. Let \bar{J} be the preimage in \bar{A} of that ideal. Then \bar{J} is the ideal whose existence is asserted in (1).

(2): Let

$$\bar{} : A \rightarrow \bar{A}$$

be the canonical homomorphism. Write $h[\lambda] = \alpha\mathbb{1} + \lambda q[\lambda]$, with $0 \neq \alpha \in \mathbb{F}$. Then $h[\sigma] = \alpha\mathbb{1} + \sigma q[\sigma]$. We have

$$\bar{0} = \overline{h[\sigma]x} = \alpha\bar{x} + \overline{\sigma q[\sigma]x}, \text{ for all } x \in A.$$

Let $e := \sigma(-\alpha^{-1}q[\sigma]) \in A$. Then we see that $\bar{e} = \overline{\sigma(-\alpha^{-1}q[\sigma])}$ is the identity element of \bar{A} and \bar{A} is unital. Further

$$\bar{e} = \overline{(a-b)(a-b)(-\alpha^{-1}q[\sigma])}$$

(recall that $\sigma = (a-b)^2$), and we see that $\overline{(a-b)}$ is invertible in \bar{A} , so also $\bar{\sigma}$ is invertible in \bar{A} .

Finally we have $h[\bar{\sigma}] = h[\bar{\sigma}]\bar{e} = \overline{h[\sigma]e} = \bar{0}$, so the last part of (2) holds.

(3): Suppose that $g[\lambda] = \lambda - 1$. Then the ideal $\bar{I} := A(\sigma - 1)/Ah[\sigma]$ is a nilpotent ideal in \bar{A} and the image of σ in \bar{A}/\bar{I} is the identity of this algebra. As in (1) we can apply Theorem 1.1(5) to obtain the ideal \bar{J} , and (3) holds.

(4): Assume now that $g[\lambda]$ is relatively prime to $\lambda(\lambda - 1)$. We show that $\bar{\sigma} - \bar{\sigma}^2$ is invertible in \bar{A} . Let $u[\lambda], v[\lambda] \in \mathbb{F}[\lambda]$ such that

$$u[\lambda](\lambda - 1) + v[\lambda]h[\lambda] = 1.$$

Multiplying by λ we get that $u[\lambda]\lambda(\lambda - 1) + v[\lambda]\lambda h[\lambda] = \lambda$. Substituting σ for λ we see that $u[\sigma]\sigma(\sigma - 1) + v[\sigma]\sigma h[\sigma] = \sigma$. Hence $\overline{u[\sigma](\sigma^2 - \sigma)} = \bar{\sigma}$. Since $\bar{\sigma}$ is invertible in \bar{A} we see that $\bar{\sigma}^2 - \bar{\sigma}$ is invertible in \bar{A} . Now Theorem 1.1(6) completes the proof of (4). \square

Notation 3.4. If B is an algebra generated by two idempotents e and f , we denote by $\sigma_B := (e - f)^2$ (here e and f are understood from the context).

As a corollary to Proposition 3.3 we get the following theorem, which handles the case where σ is algebraic over \mathbb{F} :

Theorem 3.5. *Suppose that σ is algebraic over \mathbb{F} . Then A is a direct product of algebras $B_0 \times B_1 \times \cdots \times B_m$ such that if we denote by a_{B_i}, b_{B_i} the image of a, b in B_i , then we have*

- (1) B_i is generated by the idempotents a_{B_i}, b_{B_i} .
- (2) B_i is unital for $i \geq 1$.
- (3) $B_0 = 0$, or σ_{B_0} is nilpotent and B_0 contains a nilpotent ideal J_0 such that B_0/J_0 is commutative.
- (4) $B_1 = 0$, or $h[\sigma_{B_1}] = 0$, where $h[\lambda] = (\lambda - 1)^k$, $k \geq 1$. Furthermore B_1 contains a nilpotent ideal J_1 such that B_1/J_1 is commutative.
- (5) For $i \geq 2$, we have $h[\sigma_{B_i}] = 0$, where $h[\lambda] = g[\lambda]^k$, $k \geq 1$, and where $g[\lambda] \in \mathbb{F}[\lambda]$ is an irreducible polynomial relatively prime to $\lambda(\lambda - 1)$. Furthermore $B_i \cong M_2(\mathbb{F}[\sigma_{B_i}])$.

Proof. Write the monic minimal polynomial $m[\lambda]$ of σ over \mathbb{F} as

$$m[\lambda] = \lambda^{k_1}(\lambda - 1)^{k_2}g_3[\lambda]^{k_3} \cdots g_m[\lambda]^{k_m},$$

with g_3, \dots, g_m monic, irreducible, pairwise distinct and distinct from λ and $\lambda - 1$, and where we allow $k_i = 0$, for $i = 1$ or $i = 2$.

By a repeated application of Lemma 3.2 we see that

$$A \cong A/A\sigma^{k_1} \times A/A(\sigma - \mathbb{1})^{k_2} \times A/A(g_3[\sigma])^{k_3} \times \cdots \times A/A(g_m[\sigma])^{k_m}.$$

Now the theorem follows from Proposition 3.3. \square

Lemma 3.6. *Assume that σ is transcendental over \mathbb{F} . Then*

- (1) (Bergman [B, §12.2]) *A is a free module over $\mathbb{F}[\sigma]$ with basis σ, a, b, ab ;*
- (2) *there is an involution $*$ on A as defined in Theorem 1.1(8).*

Proof. First note that if $g[\lambda] \in \mathbb{F}[\lambda]$ is a polynomial which is not a scalar (i.e., $g \notin \mathbb{F}$), then $Ag[\sigma] \neq A$. This follows from Proposition 3.1.

Suppose $f_1[\sigma]\sigma + f_2[\sigma]a + f_3[\sigma]b + f_4[\sigma]ab = 0$. Let $g[\lambda] \in \mathbb{F}[\lambda]$ be an irreducible polynomial prime to $\lambda(\lambda - 1)$ and to f_1, \dots, f_4 . Consider $B := A/Ag[\sigma]$. It is a nontrivial algebra, so by Proposition 3.3(4), $B \cong M_2(\mathbb{F}[\sigma_B])$. Clearly $\mathbb{F}[\sigma_B]$ is a field, so since B is 4-dimensional over $\mathbb{F}[\sigma_B]$ and is spanned by the images of σ, a, b, ab (Theorem 1.1(2)), we get a contradiction. This shows (1) and (2) follows from (1) and Theorem 1.1(8). \square

REFERENCES

- [B] G. Bergman *Modules over coproducts of rings*, Transactions of the American Mathematical Society **200** (1974), 1–32.
- [DeMR] T. De Medts, F. Rehren, *Jordan algebras and 3-transposition groups*, <https://arxiv.org/abs/1502.05657>.
- [HRS1] J. I. Hall, F. Rehren, S. Shpectorov, *Universal axial algebras and a theorem of Sakuma*, J. Algebra **421** (2015), 394–424.
- [HRS2] J. I. Hall, F. Rehren, S. Shpectorov, *Primitive axial algebras of Jordan type*, J. Algebra **437** (2015), 79–115.
- [HSS] J. I. Hall, Y. Segev, S. Shpectorov, *Miyamoto involutions and axial algebras of Jordan type half*, preprint.
- [Her] I. N. Herstein, *Noncommutative rings*, The Carus Mathematical Monographs, No. 15 Published by The Mathematical Association of America; distributed by John Wiley & Sons, Inc., New York 1968.
- [I] A. A. Ivanov, *The Monster Group and Majorana Involutions*, Cambridge Tracts in Mathematics, vol. **176**, 2009.
- [J] N. Jacobson, *Structure and representations of Jordan algebras*, American Mathematical Society Colloquium Publications, Vol. XXXIX American Mathematical Society, Providence, R.I. 1968.
- [Ja] S. K. Jain, *Prime rings having one-sided ideal with polynomial identity coincide with special Johnson rings*, J. Algebra **19** (1971) 125–130.
- [L] T.J. Laffey, *Algebras generated by two idempotents*, Linear Algebra Appl. **37** (1981), 45–53.
- [Ma] A. Matsuo, *3-Transposition groups of symplectic type and vertex operator algebras*, J. Math. Soc. Japan **57** (2005) 639–649.
- [Mi] M. Miyamoto, *Griess algebras and conformal vectors in vertex operator algebras*, J. Algebra **179** (1996) 523–548.
- [R] L.H. Rowen, *Graduate algebra: Noncommutative view*, AMS Graduate Studies in Mathematics **91**, 2008.
- [Sa] S. Sakuma, *6-Transposition property of τ -involutions of vertex operator algebras*, Int. Math. Res. Not. IMRN 2007, no. 9, rnm030, 19pp.

- [ZSSS] K. A. Zhevlakov, A. M. Slinko, I. P. Shestakov, A. I. Shirshov, *Rings that are nearly associative*, translated from the Russian by Harry F. Smith. Pure and Applied Mathematics, **104**. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], New York-London, 1982. xi+371 pp.
- [V] I. Vais, *Algebras that are generated by two idempotents*, (Russian) Seminar Analysis (Berlin, 1987/1988), 139–145, Akademie-Verlag, Berlin, 1988.

LOUIS ROWEN, DEPARTMENT OF MATHEMATICS, BAR-ILAN UNIVERSITY, RAMAT GAN, ISRAEL

E-mail address: `rowen@math.biu.ac.il`

YOAV SEGEV, DEPARTMENT OF MATHEMATICS, BEN-GURION UNIVERSITY, BEER-SHEVA 84105, ISRAEL

E-mail address: `yoavs@math.bgu.ac.il`